REMARKS

Favorable reconsideration of the application is respectfully requested in light of the amendments and remarks herein.

Upon entry of this amendment, claims 1-6 and 8-18 will be pending. By this amendment, claims 1, 8, and 13 have been amended. No new matter has been added.

§103 Rejection of Claims 1, 6, and 13

In Section 7 of the Office Action, claims 1, 6, and 13 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Bruce Schneier's Applied Cryptography (hereinafter referred to as "Schneier") in view of Sasaki et al. (U.S. Patent 6,378,071; hereinafter referred to as "Sasaki"). Claims 1, 8, and 13 have been amended to address the rejection.

Conventionally, when encrypting compressed data and recording it in a storage medium, the compression blocks and encryption blocks usually do not match. Therefore, when reading data from the storage medium in units of a compression block, part of the data in an encryption block sometimes is not read out and accurate decryption can no longer be performed. Further, when editing data recorded in a storage medium, for example, data is divided and combined in units of a compression block. In this case, there is a good possibility that part of the data of the encryption block will no longer be included in the edited data and accurate decryption may not be possible.

To solve the above-described problem of the conventional encryption/compression techniques, embodiments of the present invention include apparatus, system, and method for efficiently encrypting data.

For example, the structure of data processing apparatus claim 1, as presented herein, includes:

"A data processing apparatus comprising:

encrypting means for encrypting data in units of an encryption block having a predetermined data length;

processing means for defining a <u>plurality of processing blocks, each</u> processing block having a data block length of a whole multiple of said predetermined length of said encryption block and for expanding compressed data in units of said predetermined processing block length,

<u>wherein said encryption block is configured to not straddle any of said plurality of processing blocks</u>;

storage means for storing the encrypted data; and

control means for writing the encrypted data in said storage means so that the data positioned in the same encryption block is also positioned in the same processing block, said control means reading the data from said storage means in units of the processing block."

(emphasis added)

Accordingly, in one aspect of claim 1, the processing means defines a plurality of processing blocks, each processing block having a data block length of a whole multiple of the predetermined length of the encryption block and for expanding compressed data in units of the predetermined processing block length, wherein the encryption block is configured to not straddle any of the plurality of processing blocks. This limitation is disclosed in the *Specification, page29, lines 1-5*. "In the present embodiment, the number of bytes (for example 160 bytes) of the sound unit SU is made a whole multiple of the number of bytes (for example 8 bytes) of a cipher block, that is, the unit of encryption. Namely, one sound unit SU is comprised of, for example, 20 cryptograms Ci. Each cryptogram Ci is located within a sound unit SU, and

a cryptogram Ci never straddles a plurality of sound units SUs."

By contrast, neither Schneier nor Sasaki teach or suggest defining a plurality of processing blocks, each processing block having a data block length of a whole multiple of the predetermined length of the encryption block and for expanding compressed data in units of the predetermined processing block length, wherein the encryption block is configured to not straddle any of the plurality of processing blocks. Therefore, Schneier and Sasaki, individually or in combination, fail to teach or suggest all the limitations of claim 1.

Based on the foregoing discussion, claim 1 should be allowable over Schneier and Sasaki. Since claim 13 closely parallels, and recites substantially similar limitations as recited in, claim 1, claim 13 should also be allowable over Schneier and Sasaki. Further, since claim 6 depends from claim 1, claim 6 should also be allowable over Schneier and Sasaki.

Accordingly, it is submitted that the rejection of claims 1, 6, and 13 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 2-3, 14-15, and 18

In Section 10 of the Office Action, claims 2-3, 14-15, and 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Sasaki, and in further view of Bellovin *et al.* (U.S. Patent 5,241,599; hereinafter referred to as "Bellovin").

Based on the foregoing discussion regarding claims 1 and 13, and since claims 2-3, 14-15, and 18 depend from one of claims 1 and 13, claims 2-3, 14-15, and 18 should also be allowable over Schneier and Sasaki. Further, since Bellovin was merely cited for teaching the insertion of data in order to meet the predetermined length of block, it is maintained that

Schneier, Sasaki, and Bellovin, individually or in combination, fail to teach or suggest all the limitations of claims 2-3, 14-15, and 18.

Accordingly, it is submitted that the rejection of claims 2-3, 14-15, and 18 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 4 and 16

In Section 13 of the Office Action, claims 4 and 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier, Sasaki, and Bellovin, and in further view of Cassagnol (U.S. Patent 6,385,727).

Based on the foregoing discussion regarding claims 1 and 13, and since claims 4 and 16 depend from claims 1 and 13, respectively, claims 4 and 16 should also be allowable over Schneier, Sasaki, and Bellovin. Further, since Cassagnol was merely cited for teaching the storing of values initially used when encrypting stored in one of the processing blocks, it is maintained that Schneier, Sasaki, Bellovin, and Cassagnol, individually or in combination, fail to teach or suggest all the limitations of claims 4 and 16.

Accordingly, it is submitted that the rejection of claims 4 and 16 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 5 and 17

In Section 14 of the Office Action, claims 5 and 17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier, Sasaki, Bellovin, and Cassagnol, and in further

view of Yuenyongsgool (U.S. Patent 6,202,152).

Based on the foregoing discussion regarding claims 1 and 13, and since claims 5 and 17

depend from claims 1 and 13, respectively, claims 5 and 17 should also be allowable over

Schneier, Sasaki, Bellovin, and Cassagnol. Further, since Yuenyongsgool was merely cited for

teaching the storage of data by consecutive addresses, it is maintained that Schneier, Sasaki,

Bellovin, Cassagnol, and Yuenyongsgool, individually or in combination, fail to teach or suggest

all the limitations of claims 5 and 17.

Accordingly, it is submitted that the rejection of claims 5 and 17 based upon 35 U.S.C.

§103(a) has been overcome by the present remarks and withdrawal thereof is respectfully

requested.

§103 Rejection of Claim 8

In Section 15 of the Office Action, claim 8 stands rejected under 35 U.S.C. §103(a) as

being unpatentable over Schneier in view of Sasaki, and in further view of Bahout *et al.* (U.S.

Patent 5,594,793; hereinafter referred to as "Bahout").

Based on the foregoing discussion regarding claim 1, and since claim 8 closely parallels,

and recites substantially similar limitations as recited in, claim 1, claim 8 should also be

allowable over Schneier and Sasaki. Further, since Bahout was merely cited for teaching a

system for mutual identification between the storage and data processing apparatuses, it is

maintained that Schneier, Sasaki, and Bahout, individually or in combination, fail to teach or

suggest all the limitations of claim 8.

Accordingly, it is submitted that the rejection of claim 8 based upon 35 U.S.C. §103(a)

has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 9 and 10

In Section 16 of the Office Action, claims 9 and 10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Sasaki and Bahout, and in further view of Bellovin.

Based on the foregoing discussion regarding claim 8, and since claims 9 and 10 depend from claim 8, claims 9 and 10 should also be allowable over Schneier, Sasaki, and Bahout. Further, since Bellovin was merely cited for teaching the insertion of data in order to meet the predetermined length of block, it is maintained that Schneier, Sasaki, Bahout, and Bellovin, individually or in combination, fail to teach or suggest all the limitations of claims 9 and 10.

Accordingly, it is submitted that the rejection of claims 9 and 10 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claim 11

In Section 19 of the Office Action, claim 11 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Sasaki, Bahout, Bellovin, and in further view of Cassagnol.

Based on the foregoing discussion regarding claim 10, and since claim 11 depends from claim 10, claim 11 should also be allowable over Schneier, Sasaki, Bahout, and Bellovin. Further, since Cassagnol was merely cited for teaching the storing of values initially used when encrypting stored in one of the processing blocks, it is maintained that Schneier, Sasaki, Bahout, Bellovin, and Cassagnol, individually or in combination, fail to teach or suggest all the

limitations of claim 11.

Accordingly, it is submitted that the rejection of claim 11 based upon 35 U.S.C. §103(a)

has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claim 12

In Section 20 of the Office Action, claim 12 stands rejected under 35 U.S.C. §103(a) as

being unpatentable over Schneier in view of Sasaki, Bahout, Bellovin, and Cassagnol, and in

further view of Yuenyongsgool.

Based on the foregoing discussion regarding claim 11, and since claim 12 depends from

claim 11, claim 12 should also be allowable over Schneier, Sasaki, Bahout, Bellovin, and

Cassagnol. Further, since Yuenyongsgool was merely cited for teaching the storage of data by

consecutive addresses, it is maintained that Schneier, Sasaki, Bahout, Bellovin, Cassagnol, and

Yuenyongsgool, individually or in combination, fail to teach or suggest all the limitations of

claim 12.

Accordingly, it is submitted that the rejection of claim 12 based upon 35 U.S.C. §103(a)

has been overcome by the present remarks and withdrawal thereof is respectfully requested.

Conclusion

In view of the foregoing, entry of this amendment, and the allowance of this application

with claims 1-6 and 8-18 are respectfully solicited.

In regard to the claims amended herein and throughout the prosecution of this

application, it is submitted that these claims, as originally presented, are patentably distinct over

the prior art of record, and that these claims were in full compliance with the requirements of 35

U.S.C. §112. Changes that have been made to these claims were not made for the purpose of

patentability within the meaning of 35 U.S.C. §§101, 102, 103 or 112. Rather, these changes

were made simply for clarification and to round out the scope of protection to which Applicant is
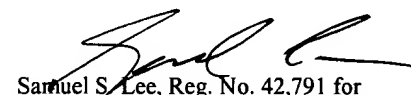
entitled.

In the event that additional cooperation in this case may be helpful to complete its

prosecution, the Examiner is cordially invited to contact Applicant's representative at the

telephone number written below.

The Commissioner is hereby authorized to charge any insufficient fees or credit any

overpayment associated with the above-identified application to Deposit Account 50-0320.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP

By: Samuel S. Lee, Reg. No. 42,791 for
William S. Frommer
Reg. No. 25,506
(212) 588-0800